UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/752,420	01/05/2004	Gregory Gordon Rose	030010	3858

23696 7590 10/24/2007
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
KANE, CORDELIA P	
ART UNIT	PAPER NUMBER
2132	
NOTIFICATION DATE	DELIVERY MODE
10/24/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

Office Action Summary	**Application No.** 10/752,420	**Applicant(s)** ROSE ET AL.	
	Examiner Cordelia Kane	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments, see Remarks, filed September 24, 2007, with respect to the rejections of claims 3 – 13, 19 – 21, 26 – 28, 33 – 42, 47 – 49, and 51 have been fully considered and are persuasive.. Therefore, the rejection has been withdrawn. However, upon further search and discovering of new prior art, a new grounds' of rejection are made.

2. Regarding arguments for claims 1, 2, 14 – 18, 22 – 25, 29 – 32, 43 – 46, and 50, applicant's arguments have been fully considered but they are not persuasive. In response to applicant's argument that the device is "operational in a mobile device", a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art.. If the prior art structure is capable of performing the intended use, then it meets the claim.

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

4. Claims 1, 14, 22 and 50 are rejected under 35 U.S.C. 102(e) as being anticipated by Robert L. Hollis et al's US Patent 6,959,393. Referring to claims 1, 14 and 22, Hollis teaches:

a. Creating a first and second private and public key pair (column 24, lines 39-40).

b. Both the second public and private key are outputted (column 24, line 41)

c. It is inherent that the first private key would be used for authentication since it is not the backup. Also, it is specifically stated that it is used for authentication (column 8, lines 59-60).

5. Referring to claim 50, Hollis teaches:

a. A processor for creating a first and second private and public key pair (column 24, lines 39-40).

b. A storage medium to store the first private key (column 9, line 55).

c. A transmitter to output the second private and public key pair (column 24, line 41) at the same time as the first public key (column 24, lines 43-44).

d. Using the first private key for authenticating is inherent from the fact that it is not the backup.

6. Claims 29, 30, 43 and 44 are rejected under 35 U.S.C. 102(e) as being anticipated by Joerg Schwenk's US Patent 7,162,037. Referring to claims 29 and 43, Schwenk teaches:

d. Creating a private (v) and public key (V) using a system parameter (g) (column 4, line 43)

e. Outputting the public key and the system parameter (column 4, lines 43-45). While it is not specifically stated that g is outputted, both entities have it so it can be inferred that it was outputted.

f. The private key v is used to create the public key V, therefor it is used for authentication. The authentication of the recipient takes place when the private key is used to decrypt the message (column 1, lines 40-41). This way the recipient knows it was the intended recipient of the message.

7. Referring to claims 30 and 44, Schwenk teaches:

g. Creating a new private key C using the previous private key v and the system parameter (column 4, lines 56-59). The system parameter g is used to calculate R and therefor S, which is then used to calculate C.

h. The secret key is used for authentication (column 4, line 53-54).

Claim Rejections - 35 USC § 103

8. Claims 2, 15 – 18, and 23 – 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollis and further in view of Bruce Schneier's Applied Cryptography. Referring to claims 2, 15 and 23, Hollis teaches all the limitations of the parent claim, but fails to teach the splitting of the second public key into shares. Schneier goes on to teach that it is the best method to split the key into pieces and share the key between

different entities (page 182, 1st and 2nd paragraph). It would have been obvious to modify Hollis to separate the backup key into different parts and distribute to different entities, as taught by Schneier, because it is more secure, since the key is protected against malicious attacks (page 182, paragraph 2).

9. Referring to claims 16, and 24, Hollis teaches using the second private key for authentication (column 10, line 23). It fails to teach the recreation of the second private key. Schneier teaches that separating the keys is a better way to secure backup keys and that when it comes time to use them that you have to reconstruct them (page 182 second paragraph). It would have been obvious to modify Hollis to reconstruct the keys, as taught by Schneier, because it is a more secure way to store the backup key since it is protected against malicious attacks (page 182, paragraph 2).

10. Referring to claim 17, Hollis teaches the creation of a primary key and a backup key (column 24, lines 39-41). It would have been obvious to modify Hollis to create a third private and public key pair, once the backup key had been used since there would need to be a new backup. It also would have been obvious to then distribute the new backup public key, and since it is an offline backup (column 24, line 41) it would have to have been outputted.

11. Referring to claim 18, Hollis teaches the creation of a primary key and a backup key (column 24, lines 39-41). It would have been obvious to modify Hollis to create a third private and public key pair, once the backup key had been used since there would need to be a new backup. It would also be obvious to repeat that process again and create a fourth backup pair of keys once the other backup pair of keys had been used.

Both new public keys would then need to be outputted, since the backup is stored as an offline backup (column 24, lines 41) it would need to be outputted. Schneier teaches distributing pieces of a private key to be used for recreation later (page 182, second paragraph). Since the fourth key pair would now be the backup, it would have been obvious to modify Hollis so that it distributes pieces of the fourth private key for recreation later since it is a more secure way to store backups, since it protects the key against malicious attacks (page 182, paragraph 2).

12. Referring to claim 25, Hollis teaches disabling the first private key when the second is used for authentication (column 14, lines 46-48).

13. Claims 11 – 13, 19 – 21, 26 – 28, and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollis in view of Gregory O'Shea et al's US Publication 2002/0152380 A1. Hollis discloses:

e. Receiving a first public key (column 9, lines 63-64).

f. Receiving a second public key (column 10, lines 33-34).

g. Using the first public key for authentication (column 14, lines 38-40, column 8, lines 59-60).

h. Using the second public key for authentication if the first public key fails (column 10, lines 31-36).

14. Hollis does not explicitly disclose receiving the public keys from the mobile user device, and authenticating the mobile user device. However, O'Shea discloses outputting the public key (page 2, paragraph 9), and then authenticating using the

public-private key pair (page 1, paragraph 8). Hollis and O'Shea are analogous art because they are from the same field of endeavor, encryption keys. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hollis and O'Shea before him or her, to modify the key system of Hollis to include the mobile devices of O'Shea. The suggestion/motivation for doing so would have been so the recipient can authenticate the information based only on the data provided (page 1, paragraph 8).

15. Referring to claims 12, 20 and 27, Hollis teaches the creation of a primary key and a backup key (column 24, lines 39-41). It would have been obvious to modify Hollis to create a third private and public key pair, once the backup (second) key had been used, as taught by Hollis (column 10, line 23), since there would need to be a new backup. It would have been obvious that after creation of the new backup key pair to distribute the new (third) public key since it would be needed for future authentication.

16. Referring to claims 13, 21, and 28, Hollis teaches the creation of a primary key and a backup key (column 24, lines 39-41). It would have been obvious to modify Hollis to create a third private and public key pair, once the backup key had been used since there would need to be a new backup. It would also be obvious to repeat that process again and create a fourth backup pair of keys. It would have been obvious to then distribute the third and fourth public keys since they would be needed for future authentication.

17. Referring to claim 51, Hollis teaches:

i. Receiving a first public key (column 9, lines 64-65) and a second public key (column 10, lines 33-34).

j. A storage medium for storing both the first and second public keys (column 9, lines 59-61).

k. A processor that knows to use the second public key when the first key fails (column 10, lines 35-36). Using the first public key for authentication is inherent from it not being the backup key.

18. Hollis does not explicitly disclose receiving the public keys from the mobile user device, and using the public keys for authentication of the mobile user device. However, O'Shea discloses outputting the public key (page 2, paragraph 9), and then authenticating using the public-private key pair (page 1, paragraph 8). Hollis and O'Shea are analogous art because they are from the same field of endeavor, encryption keys. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hollis and O'Shea before him or her, to modify the key system of Hollis to include the mobile devices of O'Shea. The suggestion/motivation for doing so would have been so the recipient can authenticate the information based only on the data provided (page 1, paragraph 8).

19. Claims 31, 32, 45, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwenk and further in view of Liao et al's US Patent 6,263,437. Referring to claims 31 and 45, Schwenk teaches the limitations of the parent claim. It fails to teach the use of a counter value. Liao teaches the use of a counter value to keep

track of the generations of key regeneration (column 15, line 59-61). It would have been obvious to modify Schwenk to include a counter value, as taught by Liao, because it would be more efficient to keep track of how many iterations have been through (column 15, lines 59-61).

20. Referring claims 32 and 46, Schwenk teaches:

i. Creating a new private key C using the previous private key v and the system parameter (column 4, lines 56-59). The system parameter g is used to calculate R and therefor S, which is then used to calculate C.

j. The secret key is used for authentication (column 4, line 53-54).

21. Schwenk fails to teach using a counter in the calculation. Liao teaches the use of a counter value to keep track of the generations of key regeneration (column 15, line 59-61). It would have been obvious to modify Schwenk to include a counter value, as taught by Liao, because it would be more efficient to keep track of how many iterations have been through (column 15, lines 59-61).

22. Claims 33, 34, 36, 37, 40, 41, 47 and 48 are rejected under 35 USC 103 (a) as being obvious over Schwenk in view of Gregory O'Shea et al's US Publication 2002/0152380 A1. Referring to claims 33, 40 and 47, Schwenk discloses:

k. Receiving a public key V, and a system parameter g (column 4, lines 43-45).

l. Generating a new public key U using the seed value S after the loss of a key (column 3, lines 59-61). The seed value S is derived from the system parameter g and the public key V, therefor the public key and system parameter are used to generate the new public key. It is inherent that the public key would have failed otherwise the system would not know that the key had been lost (column 4, line 55).

23. Schwenk does not explicitly disclose that the keys are received from the mobile user device. However, O'Shea discloses the mobile device outputting the public key (page 2, paragraph 9). Schwenk and O'Shea are analogous art because they are from the same field of endeavor, encryption keys. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Schwenk and O'Shea before him or her, to modify key regeneration system of Schwenk to be on the mobile device of O'Shea. The suggestion/motivation for doing so would have been to be able to reconstruct the key in the event it is lost (Schwenk, column 5, line 55).

24. Referring to claims 34, 41 and 48,, Schwenk teaches generating a new public key U using the seed value S (column 2, lines 59-63) which is derived using powers of the previous public key V (Figure 1). It is inherent that the public key that works would be accepted.

25. Referring to claim 36, Schwenk teaches:

m. Creating a private (v) and public key (V) using a system parameter (g) (column 4, line 43)

n. Outputting the public key and the system parameter (column 4, lines 43-45). While it is not specifically stated that g is outputted, both entities have it so it can be inferred that it was outputted.

26. Schwenk does not explicitly disclose using the private key for authentication of the mobile user device. However, O'Shea discloses that the private key is used for authentication of the mobile device (page 1, paragraph 8). Schwenk and O'Shea are analogous art because they are from the same field of endeavor, encryption keys. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Schwenk and O'Shea before him or her, to modify key regeneration system of Schwenk to be on the mobile device of O'Shea. The suggestion/motivation for doing so would have been so the recipient can authenticate the information based only on the data provided (page 1, paragraph 8).

27. Referring to claim 37, Schwenk teaches creating a new private key C using the previous private key v and the system parameter (column 4, lines 56-59). The system parameter g is used to calculate R and therefor S, which is then used to calculate C.

28. Claims 3 – 10 are rejected under 35 USC 103 (a) as being obvious over Hollis in view of Schneier and further in view of O'Shea. Hollis teaches using the second private key for authentication (column 10, line 23). It fails to teach the recreation of the second private key. Schneier teaches that separating the keys is a better way to secure backup keys and that when it comes time to use them that you have to reconstruct them (page 182 second paragraph). It would have been obvious to modify Hollis to reconstruct the keys, as taught by Schneier, because it is a more secure way to store the backup key since it will protect it against malicious attacks (page 182, 2nd paragraph).

29. Hollis in view of Schneier fails to teach that the key is recreated at a mobile device and then used for authentication of the mobile user device. However, O'Shea teaches holding the private key (page 2, paragraph 9), and then authenticating using the public-private key pair (page 1, paragraph 8). Hollis in view of Schneier and O'Shea are analogous art because they are from the same field of endeavor, encryption. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hollis in view of Schneier and O'Shea before him or her, to modify the key system of Hollis in view of Schneier to include the mobile devices of O'Shea. The suggestion/motivation for doing so would have been so the recipient can authenticate the information based only on the data provided (page 1, paragraph 8).

30. Referring to claim 4, Hollis teaches disabling the first private key when the second is used for authentication (column 14, lines 46-48). Hollis fails to teach that the key is used for authentication of a mobile device, however O'Shea discloses that the public private key pair is used for the authentication (page 1, paragraph 8).

31. Referring to claim 5, Hollis teaches the creation of a primary key and a backup key (column 24, lines 39-41). It would have been obvious to modify Hollis to create a third private and public key pair, once the backup key had been used since there would need to be a new backup. It also would have been obvious to then distribute the new backup public key. Hollis does not disclose that the key is outputted from the mobile user device. However, O'Shea teaches that the mobile device outputs the public key (page 2, paragraph 9).

32. Referring to claim 6, Hollis teaches using the third private key for authentication (column 10, line 23). He fails to teach the outputting of the third key in separate pieces. Schneier teaches that it is a more secure method with backup keys (third key) to split it into separate parts and distribute them to different entities, which is the same as outputting it so that it can be recreated. He goes on to teach how then the pieces can then be brought back together to be recreated (page 182, second paragraph). It would have been obvious to modify Hollis to split the key into separate pieces since it is a more secure method for backup keys. Hollis fails to teach that the re-creation of the private key is done at the mobile device. However, O'Shea teaches that the private key is held at the user device (page 1, paragraph 9) and therefor would need to be recreated there.

33. Referring to claim 7, Hollis teaches disabling the original (second) private key (column 14, lines 46-48). Hollis goes on to teach using the third private key for authentication (column 10, line 23). It fails to teach the recreation of the third private key. Schneier teaches that separating the keys is a better way to secure backup keys and that when it comes time to use them that you have to reconstruct them (page 182 second paragraph). It would have been obvious to modify Hollis to reconstruct the keys, as taught by Schneier, because it is a more secure way to store the backup key. Hollis fails to teach that the disabling is done after authentication of the mobile user device. However, O'Shea teaches that the public-private key pair is used for authentication of the mobile device (page 1, paragraph 8).

34. Referring to claim 8, Hollis teaches the creation of a primary key and a backup key (column 24, lines 39-41). It would have been obvious to modify Hollis to create a third private and public key pair, once the backup key had been used since there would need to be a new backup. It would also be obvious to repeat that process again and create a fourth backup pair of keys. It would then be inherent to distribute both new public keys. Schneier teaches distributing pieces of a private key to be used for recreation later (page 182, second paragraph). Since the fourth key pair would now be the backup, it would have been obvious to modify Hollis so that it distributes pieces of the fourth private key for recreation later since it is a more secure way to store backups.

35. Referring to claim 9, Hollis teaches using a new (third) private key for authentication (column 10, line 23). He goes on to teach the disabling of the old (second) key for authentication (column 14, lines 46-48).

36. Referring to claim 10, Hollis teaches using a new (fourth) private key for authentication (column 10, line 23). It fails to teach the recreation of the fourth private key. Schneier teaches that separating the keys is a better way to secure backup keys and that when it comes time to use them that you have to reconstruct them (page 182 second paragraph). It would have been obvious to modify Hollis to reconstruct the keys, as taught by Schneier, because it is a more secure way to store the backup key.

37. Claims 35, 38, 39, 42, and 49 are rejected under 35 USC 103 (a) as being obvious over Schwenk in view of O'Shea and further in view of Liao. Referring to claims 35, 38, 42 and 49, Schwenk in view of O'Shea discloses all the limitations of the parent

claim. Schwenk in view of O'Shea does not explicitly disclose receiving a counter value. However, Liao teaches the use of a counter value to keep track of the generations of key regeneration (column 15, line 59-61). Schwenk in view of O'Shea and Liao are analogous art because they are from the same field of endeavor, encryption keys. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Schwenk in view of O'Shea and Liao before him or her, to modify the key regeneration system in a mobile device of Schwenk in view of O'Shea to include the counter values of Liao. The suggestion/motivation for doing so would have been to keep track of the amount of key regenerations (column 15, lines 59-61).

38. Referring to claim 39, Schwenk in view of O'Shea discloses all the limitations of the parent claims. Schwenk in view of O'Shea fails to teach using a counter in the calculation. Liao teaches the use of a counter value to keep track of the generations of key regeneration (column 15, line 59-61). It would have been obvious to modify Schwenk in view of O'Shea to include a counter value, as taught by Liao, because it would be more efficient to keep track of how many key regenerations have occurred (column 15, lines 59-61).

Conclusion

39. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cordelia Kane whose telephone number is 571-272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CPK

Cordelia Kane
Patent Examiner
Art Unit 2132

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100